AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of secure key exchange between a first entity and a second entity using a trusted platform module (TPM) separate from the first and second entity and having a public/private key pair, the method comprising:

generating, by the first entity, a first key, encrypting the first key with a public key of a ~~third entity~~ TPM, the TPM separate from the first and second entities and having a public/private key pair, and storing the encrypted first key in the ~~third entity~~ the TPM;

generating, by the second entity, a second key, encrypting the second key with the public key of the ~~third entity~~ TPM, and storing the encrypted second key in the ~~third entity~~ TPM;

decrypting, by the ~~third entity~~ TPM, the encrypted first key and the encrypted second key, using the ~~third entity's~~ TPM's private key to obtain the first key and the second key;

encrypting, by the ~~third entity~~ TPM, the first key using the second key, and storing the first key encrypted by the second key in the ~~third entity~~ TPM;

obtaining, by the second entity, the first key encrypted by the second key, and decrypting, using the second key, the first key encrypted by the second key.

2. (Original) The method of claim 1, further comprising encrypting content with the first key by the second entity and transferring the encrypted content from the second entity to the first entity.

3. (Original) The method of claim 1, wherein the first entity comprises a graphics device.

4. (Original) The method of claim 1, wherein the second entity comprises an application program.

5. (Canceled)

6. (Original) The method of claim 1, wherein generating the first key comprises pseudorandomly generating the first key, and generating the second key comprises pseudorandomly generating the second key.

7. (Original) The method of claim 1, wherein the first key and the second key comprise symmetric keys.

8. (Original) The method of claim 1, further comprising signaling the first entity, by the second entity, to start the key exchange.

9. (Original) The method of claim 8, wherein signaling comprises storing a value in a register resident in the first entity.

10. (Currently amended) A system for secure key exchange comprising:

a ~~third entity~~ trusted platform module (TPM) having a public/private key pair;

a first entity separate from the TPM, the first entity to generate a first key, to encrypt the first key with the public key of the ~~third entity~~ TPM, and to store the encrypted first key in the ~~third entity~~ TPM;

a second entity to generate a second key, to encrypt the second key with the public key of the ~~third entity~~ TPM, and to store the encrypted second key in the ~~third entity~~ TPM;

wherein the ~~third entity~~ TPM decrypts the encrypted first key and the encrypted second key using the ~~third entity's~~ TPM's private key to obtain the first key and the second key, encrypts the first key using the second key, and stores the first key encrypted by the second key in the ~~third entity~~ TPM; and

wherein the second entity obtains the first key encrypted by the second key from the ~~third entity~~ TPM, and decrypts, using the second key, the first key encrypted by the second key.

11. (Original) The system of claim 10, wherein the first entity comprises a graphics device.

12. (Original) The system of claim 10, wherein the second entity comprises an application program.

13. (Canceled)

14. (Currently amended) The system of claim [[13]] 10, wherein the ~~trusted platform module~~ TPM comprises a first register to store the encrypted first key, a second register to store the encrypted second key, and a third register to store the first key encrypted by the second key.

15. (Original) The system of claim 10, wherein the first key and the second key comprise pseudorandomly generated symmetric keys.

16. (Original) The system of claim 10, wherein the second entity encrypts content with the first key and transfers the encrypted content to the first device.

17. (Currently amended) The system of claim 10, wherein the ~~third entity~~ TPM comprises an input/output pin dedicated for use by the first entity, and the first entity is coupled to the dedicated input/output pin using a buried line on a printed circuit board.

18. (Currently amended) A method of secure key exchange and protected content distribution between a graphics device and an application program comprising:

pseudorandomly generating, by the graphics device, a first symmetric key, encrypting the first symmetric key with a public key of a trusted platform module (TPM), the TPM being separate from the graphics device and the application program and storing the encrypted first symmetric key in a first register in the TPM;

pseudorandomly generating, by the application program, a second symmetric key, encrypting the second symmetric key with the public key of the TPM, and storing the encrypted second symmetric key in a second register in the TPM;

decrypting, by the TPM, the encrypted first symmetric key and the encrypted second symmetric key using the TPM's private key to obtain the first symmetric key and the second symmetric key;

encrypting, by the TPM, the first symmetric key using the second symmetric key, and storing the first symmetric key encrypted by the second symmetric key in a third register in the TPM;

obtaining, by the application program, the first symmetric key encrypted by the second symmetric key from the third register, and decrypting, using the second symmetric key, the first symmetric key encrypted by the second symmetric key; and

encrypting content, by the application program, using the first symmetric key, and sending the encrypted content to the graphics device.

19. (Original) The method of claim 18, further comprising signaling the graphics device, by the application program, to start the key exchange.

20. (Original) The method of claim 19, wherein signaling comprises storing a value in a register resident in the graphics device.

21. (Original) The method of claim 18, further comprising, decrypting, by the graphics device, the encrypted content using the first symmetric key.